IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

RB

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS

Defendants.

Civil Action No: 1:10CV156 (LMB\IDFA)

FILED UNDER SEAL unseal 2/24/10

DECLARATION OF T.J. CAMPANA IN SUPPORT OF APPLICATION OF MICROSOFT CORPORATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, T.J. Campana, declare as follows:

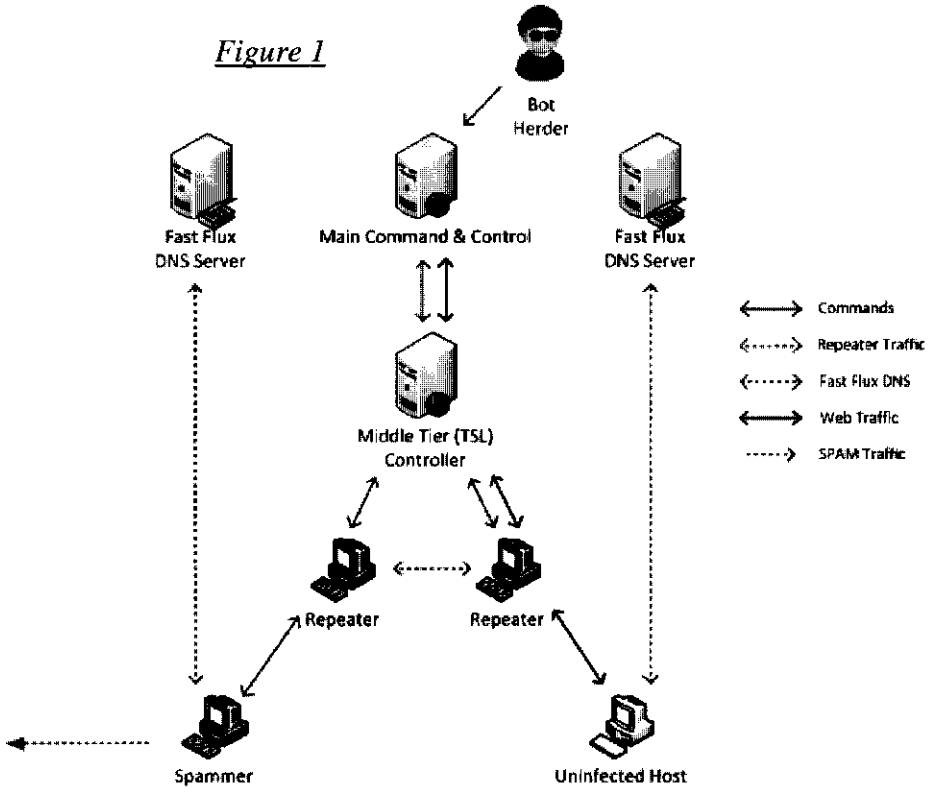
1. I am the Senior Program Manager, Security in the Digital Crimes Unit of Microsoft Corp.'s Legal and Corporate Affairs group. I make this declaration in support of the Application of Microsoft Corporation For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business. I have conducted an investigation of the structure and functions of the Waledac botnet as well as the activities carried out through the botnet, and an assessment of the impact on Microsoft's business. The Waledac botnet is causing extreme damage to Microsoft and if allowed to continue, such damage will be compounded as this case proceeds.

The Structure Of The Waledac Botnet

3. The Waledac botnet has a multi-tiered architecture, which can be represented as follows in Figure 1:

Figure 1



4. The lowest "Spammer Node" tier in this architecture is made up of infected user computers that have been determined to be behind firewalls or otherwise not directly accessible from the Internet. The botnet software placed on these infected computers sends, without the user's knowledge or permission, unsolicited bulk email (often known as "spam"). This spam email may contain code that infects further computers adding them to the botnet or may serve other purposes, such as inviting users to enter financial or other valuable personal information. The botnet selects user computers behind firewalls to act as the "Spammer Nodes" because such computers are more difficult to monitor or to reach remotely to remediate the problem. The sending of spam email is a major component of the Waledac botnet's functionality. The Waledac botnet has the capability of sending spam email to perpetuate fraud, to collect financial and personal data, to distribute harmful or fraudulent software, including fake antivirus or

"scareware" programs, to distribute questionable, potentially dangerous and unauthorized pharmaceuticals, and to carry out other similar schemes.

5. The next highest tier in the architecture, the "Repeater Node" tier, is made up of infected computers that are directly accessible from the Internet. These computers may serve several different purposes, depending on the instructions sent by the botnet's command and control computers. First, they may act as proxies relaying communications among different botnet computers, both to distribute the processing burden and to obfuscate the true source of the communications. Second, these computers may act as HTTP[1] and SOCKS 5[2] servers capable of delivering HTTP and SOCKS 5 commands and responses, when receiving requests from other botnet computers. These computers act as HTTP and SOCKS 5 "proxies" (i.e. computers that relay communications) for both infected computers already part of the botnet as well as uninfected computers that are following a URL received in a spam email message. Third, these computers may act as "DNS servers." In general, a DNS server is a computer that translates human readable hostnames or domain names (such as xinnet.com) to their corresponding binary identifier, called an IP address (such as 123.100.5.81).

6. The next highest tier in the architecture, the "TSL Servers," is the first tier that is controlled directly by the operators of the Waledac botnet and the first tier that is not made up of infected computers. The TSL Servers are "reverse proxy servers." In general, reverse proxy servers receive in-bound communications and then pass those on to additional servers. In the Waledac botnet, the TSL Servers receive in-bound communications from the Repeater Nodes and then pass them to other servers behind the TSL Servers. The purpose of TSL Servers is to obfuscate details about the servers behind them, to prevent direct communications with those servers and evade investigation of these portions of the botnet.

7. At the highest level, behind the TSL Servers, there are one or more command and

---

[1] HTTP is a primary protocol to transfer requests and information between servers and client computers on the Internet.

[2] SOCKS 5 is a newer protocol for transferring data between servers and clients.

control servers, referred to as the "Main Command & Control" servers. It is believed that this server or servers are controlled more directly by the operators of the Waledac botnet and not made up of infected computers. The Main Command & Control servers are responsible for coordinating the Waledac botnet on the whole and providing the most fundamental definitions, commands and instructions that determine how infected computers will operate and how different botnet components will interact with each other.

The Waledac Botnet: Fast Flux DNS Server

8. The Waledac botnet uses a method called "fast flux" hosting, which is a technique used by botnets to hide the location of their constituent computers by constantly changing the IP addresses of the domain names associated with the command and control and infrastructure components that make up the botnet. The purpose and result of fast flux hosting is that discovery, observation and counter-measures are made more difficult because the addressing of the constituent compromised computers is constantly changing.

9. The Waledac botnet includes a component called the "Fast Flux DNS Server." This component is a server that coordinates the domain name infrastructure associated with the Repeater Nodes thereby using a fast flux hosting technique to obfuscate the source, location, owner and other attributes of those computers. The Fast Flux DNS Server accomplishes this by regularly updating the root name servers for the various fast flux domains used by the Waledac botnet. In particular, the Fast Flux DNS Server accesses a web portal to one of the domains' registrars updating the root name servers at the registrars. To hide the location of the Fast Flux DNS Server from the registrars, all access of the server to the registrar's web portal is proxied through Repeater Node computers so there is not direct communication between the Fast Flux DNS Server and the registrar. The botnet's Fast Flux DNS Server can instruct a subset of the Repeater Nodes to act as DNS servers while the Fast Flux DNS Server reconfigures the root DNS servers to point to the configured nodes. As a result, a query by a computer to one of the Waledac domain names results in one of the Repeater nodes responding with the IP address of the queried computer or another Repeater Node computer, thereby providing the ability to

continuously obscure the attributes of these Waledac domains.

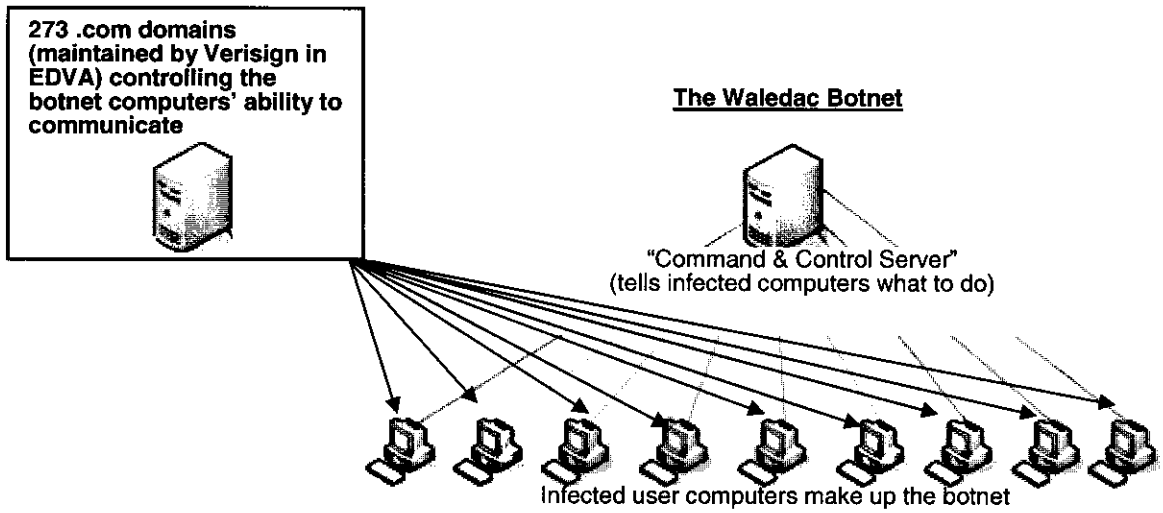
The Waledac Botnet: The Harmful Botnet Domains

10. The Waledac botnet relies upon 273 domains to support the ability of botnet nodes to communicate with each other. These 273 domains are referred to as the "Harmful Botnet Domains." I have investigated the 273 Harmful Botnet Domains. As part of my investigation, I performed lookups of these domains in a publicly accessible "WHOIS" database, which contains contact information regarding the registrants of these domains and technical details about the domains. Attached hereto as Exhibit 1 is a true and correct summary of the results of these lookups, including the 273 domain names, the registrant contact information that was provided, the domain registrars through which the registrants obtained the domains and the "top level domain" registry which ultimately maintains these domains. Each of the 273 Harmful Botnet Domains is a ".com" internet domain, which are maintained by the ".com" domain registry, Verisign, Inc., in the Eastern District of Virginia.

11. Each of the Harmful Botnet Domains is one of the foregoing described fast flux Waledac domains, representing a component in the command and control of the botnet. The computers that are part of the Waledac botnet can send "node table updates" to other computers in the botnet. These node table updates contain lists of other known Repeater Nodes, to enable and support continued communication between all of these computers. The communication from the Spammer Node tier to the Repeater Node tier and communication between Repeater Nodes depends on the accuracy of the node tables stored at each computer and depends on the accuracy of node table updates. If a node table is empty or contains invalid entries, a given botnet computer uses one of the Harmful Botnet Domains, which is hardcoded in the botnet software residing on the computer, to query the botnet for an update to the node table. Thus, the Harmful Botnet Domains continuously control the ability of the computers that make up the Waledac botnet to communicate with each other and to grow the botnet.

12. The following Figure 2 is a general representation of the relationship of the 273 Harmful Botnet Domains to the Waledac botnet:

Figure 2



13. In addition to supporting Waledac botnet's infrastructure, as described above, the Harmful Botnet Domains may further be used in at least the following way. Links to those domains may be included in unsolicited, bulk email sent out by Spammer Node computers with the purpose of spreading the botnet. For example, the Spammer Node computers have been observed to send emails indicating to the victim recipients that a news story has broken or that a loved one has sent the victim an e-card. The emails point to one of the Harmful Botnet Domains, which represents a Repeater Node computer. When the victim opens the link sent to them, in order to retrieve the story or e-card, the victim is interacting directly with the Repeater Node computer, which may deliver software that infects the victim's computer and makes it part of the Waledac Botnet. The spread of the Waledac botnet in this way is not related to any vulnerability in Microsoft's systems, but is instead achieved by misleading unwitting users into taking steps that result in the infection of their machines.

14. Attached hereto as Exhibit 2 is a true and correct copy of a document entitled "Infiltrating WALEDAC Botnet's Covert Operations: Effective Social Engineering, Encrypted HTTP2P Communications, and Fast-Fluxing Networks," by Jonell Baltazar, Joey Costoya and Ryan Flores of the security company Trend Micro. This paper describes in detail the manner in which the Waledac botnet misleads victims and causes their computers to become infected.

15. Attached hereto as Exhibit 3 are true and correct copies of excerpts from the website of security firm F-secure regarding the Waledac trojan software. This document

describes how the Waledac botnet misleads victims and causes computers to become infected.

16. Attached hereto as Exhibit 4 is a true and correct copy of a document entitled "Walowdac: Analysis of a Peer-to-Peer Botnet," by Ben Stock, Jan Göbel, Markus Engelberth Felix C. Freiling and Thorsten Holz of the Laboratory for Dependable Distributed Systems at the University of Mannheim and Secure Systems Lab at Technical University Vienna. Attached hereto as Exhibit 5 is a true and correct copy of a January 4, 2010 article entitled "Researchers Infiltrate Storm Botnet Successor: Going undercover in Waledac botnet, European researchers discover it's much bigger than they thought." The researchers whose work is reflected in these two documents have estimated that there are at least 390,000 infected user computers in the Waledac botnet during the time of their study.

17. I have recently investigated each of the Harmful Botnet Domains and have observed the operation of these domains in the context of the botnet. Based on observing the Harmful Botnet Domains, I conclude that they have no purpose other than the support and propagation of the Waledac botnet as described above and the furtherance of malicious activity through the botnet. I conclude, based on observing the content and operation of the domains, that no legitimate activity is carried out through them. When I browsed to these domains, I observed that they do not host any personal or business website content or support any legitimate business activities.

18. I have recently investigated IP addresses known to be associated with nodes and infected user computers that are part of the Waledac botnet. I collected a sampling of such IP addresses during the period December 3-21, 2009. A true and correct copy of that research is attached as Exhibit 10. Technology exists to determine the geographical location of IP addresses. Using such technology, I determined the geographical location of the Waledac IP addresses collected during the sample period. I plotted such IP addresses on maps of Virginia and the United States, to represent the location of Waledac botnet nodes, shown below in Figures 3-4. Each marker on the maps represents at least one user computer that the controllers of the Waledac botnet specifically directed malicious code toward, to infect that computer and make it

part of the botnet, and to carry out malicious activities through that computer. As can be seen, the operators of the Waledac botnet have directed such code to computers located in Virginia:

Figure 3

Infected User Computers in Virginia To Which The Waledac Botnet Delivered Malicious Code

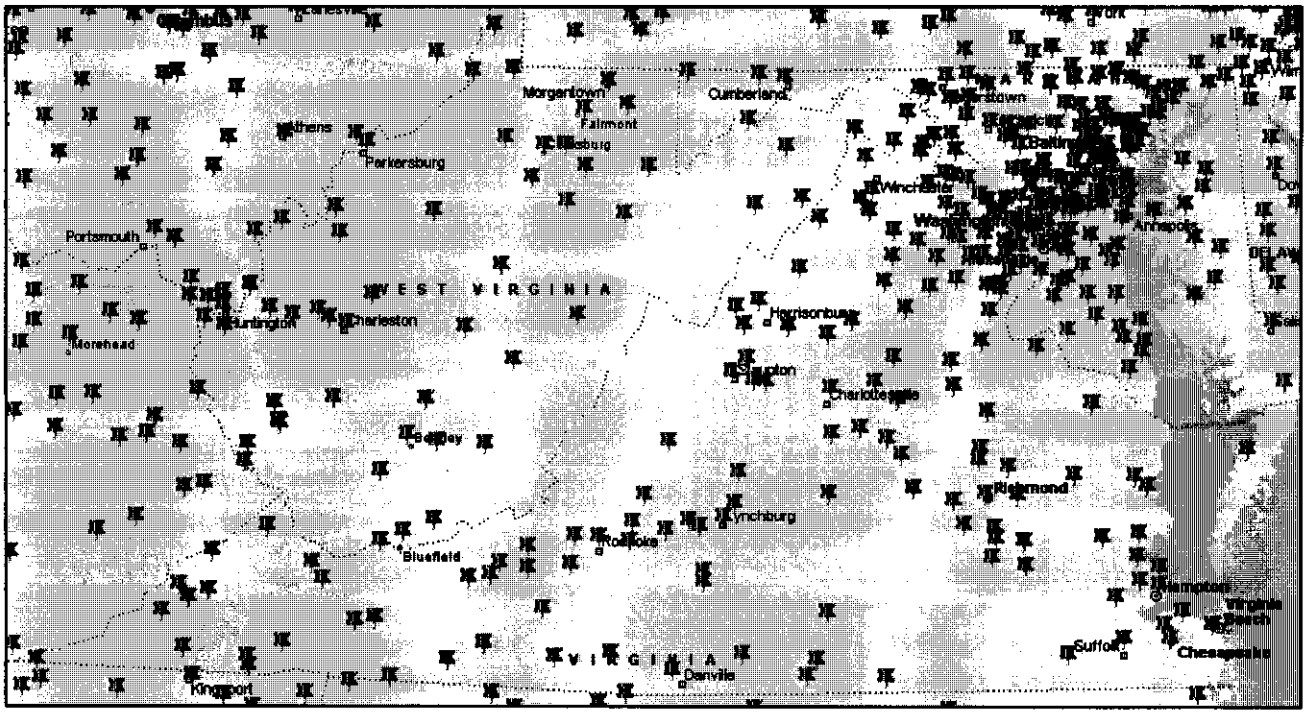
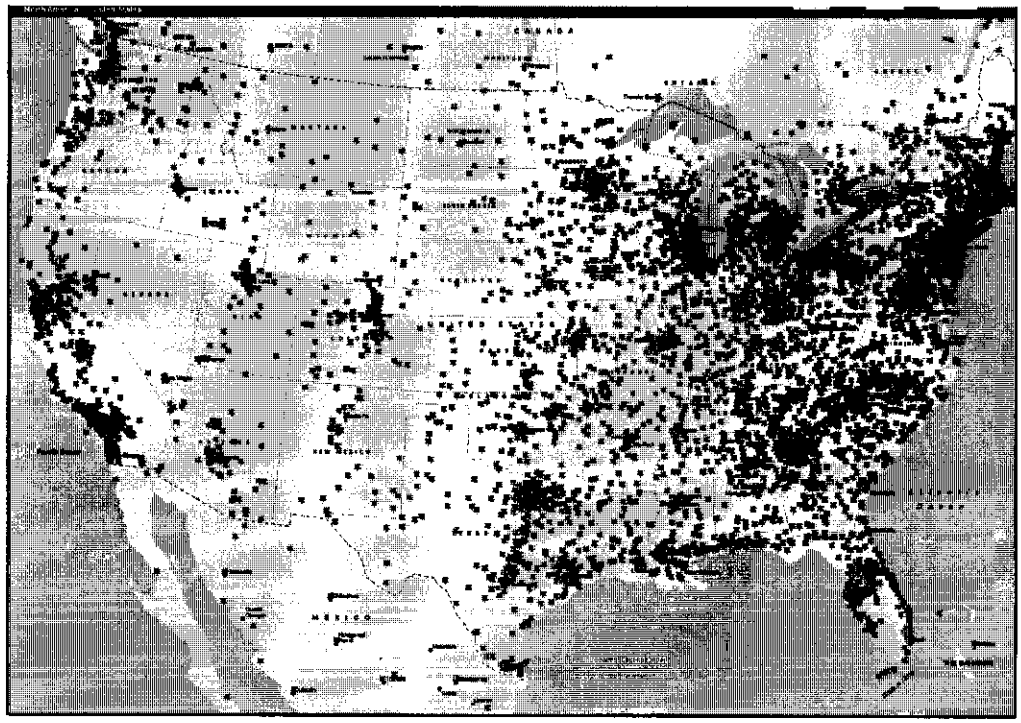


Figure 4

Infected User Computers in The U.S. To Which The Waledac Botnet Delivered Malicious Code



Overview Of Injury Caused By The Waledac Botnet To Microsoft And Its Customers

19. Microsoft is a provider of the Windows® operating system, Hotmail® e-mail services and a variety of other software and services. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Windows® and Hotmail® marks.

20. The activities carried out by the Waledac botnet, described in detail below, injure Microsoft and its reputation, brand and goodwill because users of compromised computers are likely to incorrectly believe that Microsoft is the source of computer problems caused by the botnet. Microsoft is similarly injured because the botnet directs an extraordinary amount of spam email to users of Microsoft's email services and causes spam emails to appear to originate from Microsoft. Microsoft and its customers must bear this extraordinary burden and customers are likely to incorrectly believe that Microsoft is to blame for the spam email. Microsoft receives customer support requests caused by the Waledac botnet and must expend substantial resources dealing with the injury and confusion. Microsoft has had to expend substantial resources in an attempt to assist its customers and to prevent the misperception that Microsoft is the source of damage caused by the Waledac botnet. For example, Microsoft must expend resources to clean infected computers and to block a massive amount of spam email.

21. Once customers' computers are infected and become part of the Waledac botnet, they may be unaware of that fact and may not have the technical resources to solve the problem, allowing their computers to be misused indefinitely. For example, I have reviewed the history of customer reporting relating to Waledac infections. Microsoft's Malicious Software Removal Tool has detected 131,440 instances of Waledac infected user machines. However, during the

same period in only 3110 instances did a customer affirmatively reach out to Microsoft's support website to run an online scanner and clean the computer.

22. In such circumstances, technical attempts to remedy the problem may be insufficient and the injury caused to customers will continue. The injury caused by the Waledac botnet extends far beyond Microsoft to other consumers and providers of email services and all computer users, each of whom is at risk.

23. Based on my experience assessing computer threats and the impact on business, I conclude that customers may incorrectly attribute the negative impact of the Waledac botnet to Microsoft. Further, based on my experience, I therefore conclude that there is a serious risk that customers may move from Microsoft's products and services because of the Waledac botnet and its activities. Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks.

Specific Injury Caused By The Waledac Botnet To Microsoft And Its Customers

A. Unauthorized Intrusion

24. Microsoft and its customers are injured when the Waledac botnet software is maliciously introduced onto users' computers making them part of the botnet. The malicious software that perpetuates the Waledac botnet is known by various names in the Internet security community, including: Win32/Iksmas.worm.390656 (AhnLab), Trojan.Waledac.F (BitDefender), Win32/Waledac.D (CA), Email-Worm.Win32.Iksmas.y (Kaspersky), W32/Waledac.gen (McAfee), Trj/MailStealer.F (Panda), W32/Waled-F (Sophos), W32.Waledac (Symantec), Trojan.Waledac.Gen (VirusBuster).

25. The installation of the botnet software by deceiving consumers and without Microsoft's authorization is an intrusion into the Microsoft Windows operating system, without Microsoft's authorization. The Windows operating system is licensed by Microsoft to end users. Attached hereto as Exhibit 6 is a true and correct copy the Windows 7 end-user license agreement. Attached hereto as Exhibit 9 is a true and correct copy of the Windows Vista end-user license agreement. Attached hereto as Exhibit 7 is a true and correct copy of the Windows

XP end-user license agreement.

26. Among other things, the Waledac botnet installs and runs software without the customers' or Microsoft's knowledge or consent, software to support the botnet infrastructure, software that causes the computer to act as an HTTP Proxy, an HTTP Server, a DNS Server, a SOCKS5 Proxy, software that acts as an SMTP email engine, software enabling the computer to initiate a DDoS attack, and an HTTP P2P Engine;

27. The Waledac botnet specifically targets the Windows operating system. For example, it writes particular entries to the registry of the Windows operating system, without the consent of Microsoft or its customers. For example, registry keys written by the botnet include:

- HKCU\Software\Microsoft\Windows\CurrentVersion\LastCommandId (allows botnet to know which commands to execute on a given infected machine)
- HKCU\Software\Microsoft\Windows\CurrentVersion\tsl (allows botnet to retrieve lists of known TSL Servers in order to facilitate communication between the Spammer Node and Repeater Node tiers and the higher-level tiers, particularly the Command & Control Server)
- HKCU\Software\Microsoft\Windows\CurrentVersion\FWDone (allows botnet to determine whether email harvesting functionality is already in progress or whether that computer needs to be reported up to the Command & Control Server so that instructions can be returned to the computer)
- HKCU\Software\Microsoft\Windows\CurrentVersion\MyID (this is the 16 byte ID assigned by the botnet to the infected node)
- HKCU\Software\Microsoft\Windows\CurrentVersion\Kist (this is the Encrypted/Encoded list of repeater nodes known to the node)
- HKCU\Software\Microsoft\Windows\CurrentVersion\LastCommandId (this is the last command number executed as instructed by the Command & Control Server.

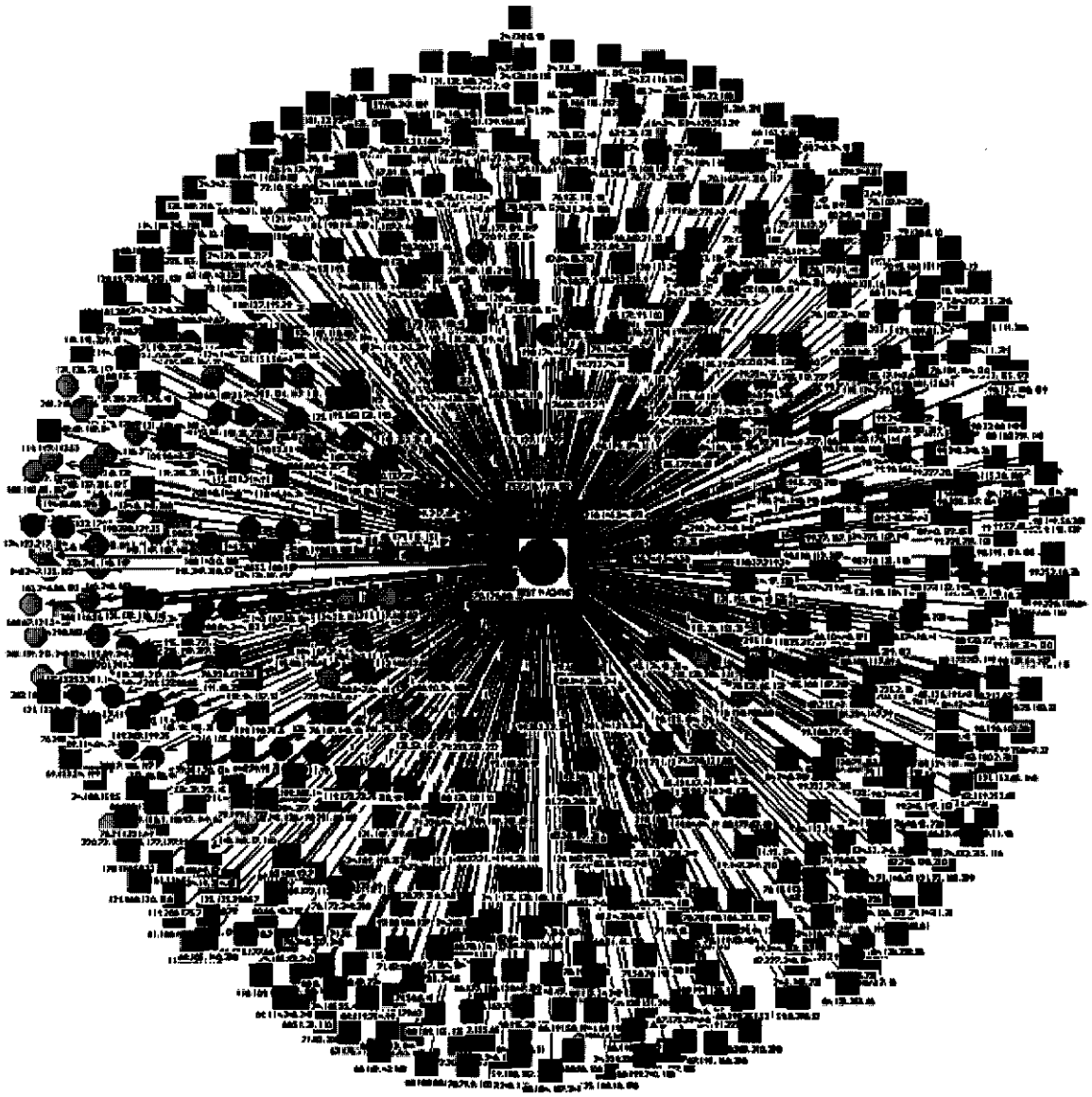
28. Once part of the botnet, the user's computer is under control of the parties controlling the botnet. They steal personal information, such as email addresses from the user's

computer. The parties controlling the botnet can cause the user's computer to send bulk, unsolicited "spam" emails, deliver malicious software to infect other computers or otherwise use it to carry out fraud, computer intrusions or other malicious and illegal conduct. These activities are further described below.

29. Once the user's computer is under the control of the parties controlling the botnet, the computer's performance may suffer significantly due to the high volume of processing, data transfer and connections to the Internet that botnet is causing the user's computer to undertake without the user's permission. I recently investigated the impact the Waledac botnet has on the performance of an infected user computer.

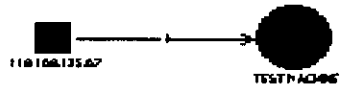
30. I first intentionally downloaded to a computer, operating under normal conditions, the malicious Waledac code that would be present on an infected user computer acting as a "Repeater" node and observed the operation of the infected machine for a period of time. With the malicious Waledac code on the computer, it made numerous requests to other computers on the Internet and also other machines on the Internet made requests from this infected machine. This significant processing activity would degrade the overall performance and tax the resources of a user computer, without their knowledge. A representation of the activity on the infected machine is set forth at Figure 6 below. Circles represent instances when the infected machine made requests from other computers on the Internet. Squares represent instances when other computers on the Internet made requests from the infected machine:

Figure 6



31. I then reset the computer to a clean state, without the malicious Waledac code present and observed the operation of the uninfected machine. During the same period of observation under normal operation of the computer, a single inbound SMTP connection occurred from the Internet. A representation of the activity in this regard is set forth at Figure 5:

Figure 5



B. Spam Email

32. Researchers have conservatively estimated that the Waledac botnet has the capacity to send 1.5 billion spam emails per day to others, including to users of Microsoft's Hotmail email service. This research is described at Ex. 4 to this declaration at p. 7 and in Ex. 5.

33. At my direction, Microsoft personnel conducted research into the amount of spam email attributable to the Waledac botnet that is sent to Microsoft's Hotmail accounts. Microsoft analyzed a sample period between December 3, 2009 and December 21, 2009. The volume of spam email in that brief sample period alone is overwhelming. During that period approximately 651 million connections attributable to the Waledac botnet were directed to Hotmail accounts, each capable of sending multiple spam emails. During that same period approximately an additional 23 million such emails reached Microsoft's Hotmail customers.

34. The following is the methodology used to determine the volume of spam email originating from the Waledac botnet. First, through its own investigation and from public sources, Microsoft maintains a list of IP addresses associated with machines that are part of the Waledac botnet. By examining the IP addresses associated with incoming email directed at Hotmail accounts, Microsoft may determine the volume and identity of email being sent to Hotmail accounts from Waledac machines and the volume of such email that reaches Hotmail users. Microsoft individually examined a sample of 2,433 such messages originating from IP addresses associated with Waledac infected computers and determined that 96.88% of those messages were spam. Applying that percentage to all incoming attempted emails and received emails from the Waledac IP addresses, Microsoft is able to estimate the amount of spam email being directed by the Waledac botnet at Microsoft's Hotmail users.

35. Using this methodology, the chart at Figure 7 sets forth results from the December 3, 2009 to December 21, 2009 sample period, including the number of unique Waledac IP addresses, the volume of spam email being sent to Hotmail addresses from Waledac IP addresses and the volume of spam emails that reached Microsoft' Hotmail customers.

Figure 7

Date	Total Waledac IP Addresses Sending Spam Email	Total Attempted Email Connections To Hotmail Addresses From Waledac IP Addresses	Total Emails From Waledac IP Addresses That Reached Hotmail Users
12/3	**11,924**	**40,467,232**	**1,204,481**
12/4	18,626	22,174,273	714,120
12/5	17,103	**28,540,548**	**725,559**
12/6	22,265	52,346,544	1,244,063
12/7	27,659	**32,194,622**	**1,419,413**
12/8	29,221	60,280,704	1,673,738
12/9	27,805	**36,128,630**	**1,440,420**
12/10	23,684	55,382,525	1,458,291
12/11	19,180	**29,803,721**	**848,750**
12/12	15,822	61,596,946	910,474
12/13	17,630	**37,440,063**	**927,230**
12/14	7,345	17,553,168	989,909
12/15	17,765	**22,765,729**	**1,279,526**
12/16	17,010	43,772,091	1,331,391
12/17	17,303	**30,364,480**	**1,170,048**
12/18	16,301	19,684,138	1,053,943
12/19	14,923	**19,473,710**	**889,370**
12/20	19,225	24,173,454	1,987,252
12/21	15,682	**16,983,712**	**2,535,731**
Total	**179,485**	**651,126,290**	**23,803,709**

36. The running of software on infected user computers to send such vast amounts of spam email causes performance degradation and misleads Microsoft's customers to incorrectly believe that Microsoft is the source of such issues. This causes injury to Microsoft.

37. The sending of vast amounts of spam email to Microsoft's Hotmail email services imposes a burden on Microsoft's servers, requires Microsoft to expend substantial resources in an attempt to defend against and mitigate this vast amount of email and misleads Microsoft's customers to incorrectly believe that Microsoft is the source of such issues. This causes injury to Microsoft. Microsoft is further injured when such email is falsely made to appear to originate from Microsoft's Hotmail email service.

38. It is my understanding that the parties controlling the botnet may profit from the Waledac botnet by sending spam email which may generate advertising revenue. It is further my

understanding that the parties controlling the botnet may profit from the Waledac botnet by selling to others the botnet's capability of sending spam email and carrying out similar activities on behalf of others.

39. The substance of the spam emails sent by the parties controlling the botnet may be false, misleading or fraudulent, may invite users to participate in illegal activities and may offer products or services that are dangerous, of questionable value or counterfeit. Such products or services could lead to injury to Microsoft's customers and may offend Microsoft's customers. Therefore, the substance of the spam email sent by the Waledac botnet causes injury to Microsoft and its customers.

40. The following summarizes the substance of spam emails sent by Waledac to Hotmail accounts during the December 3, 2009 through December 21, 2009 sample period, including offensive, fraudulent and illegal content. True and correct copies of such emails during the sample period are attached hereto as Exhibit 8.

a. **Viagra/Cialis:** Spam emails contained offers for purported male-enhancement pharmaceuticals such as Viagra or Cialis. It is believed that such offers involve fake pharmaceutical products that are not legitimate branded products, but are counterfeit, of questionable value or efficacy and potentially dangerous.

b. **Male Enhancement.** Spam emails contained general offers for purported male enhancement, without reference to specific pharmaceuticals.

c. **Imitation Goods:** Spam emails contained offers for counterfeit goods. For example, spam emails sent offers for "rolex replicas."

d. **Work from Home:** Spam emails contained offers for purported "work from home" situations, which are believed to be scams designed to defraud consumers and obtain money from them.

e. **Counterfeit/Pirated Software:** Spam emails contained offers for counterfeit and pirated software. For example, spam emails offered unauthorized copies of products such as Microsoft Windows and Adobe Photoshop.

f. **Casino:** Spam emails contained attempts to entice users to gamble in online casinos.

g. **Other Pharma:** Spam emails contained offers for pharmaceuticals such as Vicodin and Codeine. Again, it is believed that such offers involve fake products that are not legitimate, are of questionable efficacy and may be dangerous.

h. **Adult:** Spam emails contained attempts to entice users to visit and pay for access to various adult websites. Some such emails contain false statements purporting to be from a woman and attempting to convince the user to reply to the email.

i. **Penny Stock:** Spam emails contained attempts to entice users to purchase cheap stock in volume, thereby artificially increasing the price of that stock.

j. **Other:** Spam email also contained a variety of other schemes and devices as well, for example emails purporting to offer dental care, emails offering attachments that are believed to contain malicious code and emails requesting personal information.

41. The following Figure 8 summarizes a breakdown of the volume of such spam email categories during the December 3-21, 2009 sample period.

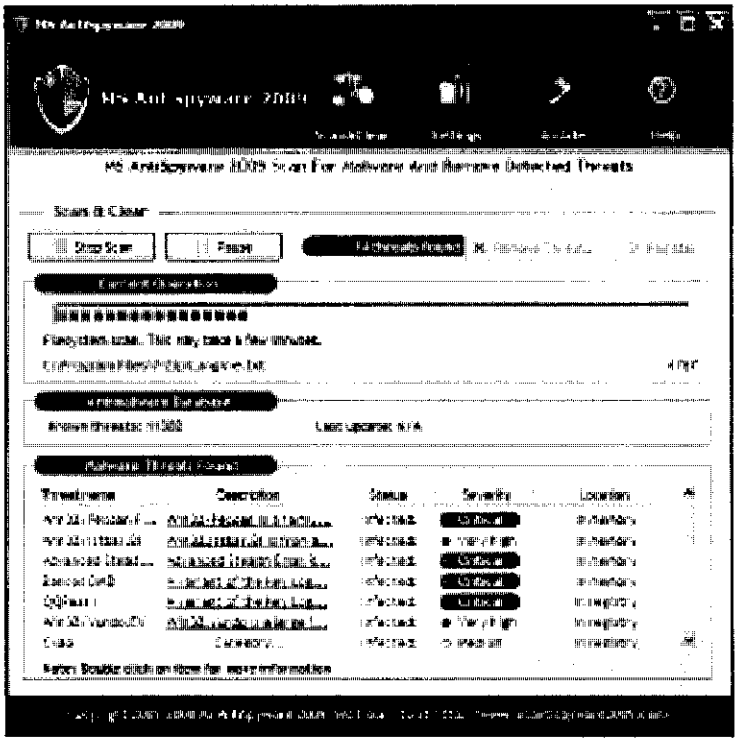
Figure 8

Date	Viagra	Male Enhancement	Imitation Goods	Work from Home	Software	Casino	Other Pharma	Adult	Penny Stock	Other
12/3	63%	11%	20%	6%	0%	0%	0%	0%	0%	0%
12/4	78%	0%	4%	0%	4%	4%	9%	0%	0%	0%
12/5	71%	17%	0%	0%	4%	0%	0%	8%	0%	0%
12/6	64%	0%	4%	0%	8%	8%	0%	8%	0%	8%
12/7	81%	0%	0%	13%	0%	0%	0%	0%	0%	6%
12/8	56%	25%	13%	0%	0%	6%	0%	0%	0%	0%
12/9	62%	8%	8%	8%	0%	0%	8%	8%	0%	0%
12/10	89%	11%	0%	0%	0%	0%	0%	0%	0%	0%
12/11	84%	0%	0%	0%	0%	4%	0%	8%	0%	4%
12/12	81%	3%	6%	0%	0%	0%	0%	0%	10%	0%
12/13	68%	0%	8%	0%	0%	5%	0%	3%	16%	0%
12/14	31%	8%	19%	0%	4%	8%	0%	8%	23%	0%

12/15	64%	5%	23%	0%	0%	0%	0%	0%	9%	0%
12/16	93%	0%	7%	0%	0%	0%	0%	0%	0%	0%
12/17	59%	0%	26%	0%	0%	15%	0%	0%	0%	0%
12/18	25%	8%	25%	0%	0%	38%	0%	4%	0%	0%
12/19	19%	0%	19%	4%	0%	41%	7%	11%	0%	0%
12/20	48%	0%	4%	11%	0%	33%	4%	0%	0%	0%
12/21	68%	0%	0%	7%	0%	21%	4%	0%	0%	0%

C. Malware

42. The Waledac botnet installs and runs fake "anti-virus" software and other similar software on infected user machines. In particular, as reflected in Exhibit 2 to this declaration at page 30, security researchers have observed that the Waledac downloads rogue antivirus software claiming to be "MS Antispyware 2009." This software is false and misleading and makes deceptive use of Microsoft's established and trusted brand, in order to deceive consumers.



43. The running of such software causes performance degradation and misleads Microsoft's customers to incorrectly believe that Microsoft is the source of such issues. This causes injury to Microsoft.

D. Unauthorized Access To And Collection Of Personal Information

44. The Waledac botnet collects and transmits personal information, including personal email address information, from users' computers. The Waledac botnet also collects information about whether such collected email addresses successfully accepted unsolicited email and which unsolicited email template was accepted by such email addresses. This enables the Waledac to collect email addresses resulting in additional spam email being sent to Microsoft's Hotmail customers. The running of such software may cause degradation of performance on the user's infected computer. Microsoft's customers may be incorrectly led to believe that Microsoft is the source of such issues. This causes injury to Microsoft.

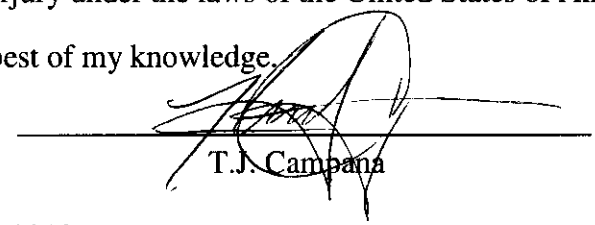
Turning Off The 273 Domains Controlling The Waledac Botnet Without First Informing The Defendants Is The Only Way To Prevent The Injury

45. The Waledac botnet is designed to resist technical mitigation efforts, eliminating viable technical means to curb the injury being caused.

46. Piecemeal requests to turn off the domains, informal dispute resolution or notice to the Defendants prior to turning off the 273 Harmful Botnet Domains, would be insufficient to curb the injury. Based on my experience observing the operation of botnets and my observations of the specific architecture of the Waledac botnet, I believe that the botnet will be moved and hidden if notice were given before turning off these domains. The parties controlling the botnet have built in fast flux infrastructure and other mechanisms designed to permit the Waledac botnet to continuously change location and to obfuscate its operations. I am specifically aware of prior instances where security researchers or the government attempted to curb injury caused by botnets, but allowed the botnet operators to receive notice. In these cases, the botnet operators immediately moved the botnet to new, unidentified locations and took other countermeasures causing the botnet to continue its operations and destroying or concealing evidence of the botnet's operations. Given the specific architecture of the Waledac botnet, I believe that, if provided advance notice that the 273 Harmful Botnet Domains were to be turned off, the operators of the Waledac botnet would take such measures just as other similarly situated botnet operators have done in the past.

47. I believe that the only way to suspend the injury caused to Microsoft, its consumers and the public is to: (1) turn off the resolution of the 273 Harmful Botnet Domains used to control the botnet at Verisign—the "top level domain" registry for .com domains—and also at the individual domain name registrars and (2) place the 273 Harmful Botnet Domains in escrow with Verisign, so that the injury is not further compounded and evidence of the misconduct can be preserved.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.



T.J. Campana

Executed this 21 day of February, 2010.